

ALGEBRA III
Práctica 1

Nota: En esta práctica anillo significa anillo conmutativo con $1 \neq 0$.

1. Sea A un anillo. Probar que:

- (i) A tiene ideales maximales y todo ideal propio I está contenido en un ideal maximal.
- (ii) P es un ideal primo si, y sólo si, A/P es dominio íntegro
- (iii) A es un cuerpo si, y sólo si, tiene exactamente dos ideales.
- (iv) \mathcal{M} es ideal maximal si, y sólo si, A/\mathcal{M} es cuerpo.

2. Probar que:

- (i) Si K es cuerpo y $f : K \rightarrow B$ es morfismo de anillos, entonces f es inyectivo.
- (ii) Si A es anillo tal que todo morfismo de anillos $f : A \rightarrow B$ es inyectivo, entonces A es un cuerpo.
- (iii) Si D es un dominio íntegro finito, entonces es cuerpo.
- (iv) \mathbb{C} no tiene subcuerpos finitos.

3. Sea $b \in \mathbb{C}$ y sea $\mathbb{Q}[b] = \{ \sum_{i=0}^n a_i b^i / a_i \in \mathbb{Q} \}$.

Probar que $\mathbb{Q}[\sqrt{2}]$, $\mathbb{Q}[i]$, $\mathbb{Q}[\sqrt[3]{2}]$ son cuerpos.

4. Caracterizar los siguientes conjuntos:

- (i) $\{ f : \mathbb{C} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos} \}$.
- (ii) $\{ f : \mathbb{Q} \rightarrow \mathbb{Z}_p, f \text{ morfismo de cuerpos} \}$.
- (iii) $\{ f : \mathbb{Q} \rightarrow \mathbb{K}, f \text{ morfismo de cuerpos} \}$, \mathbb{K} cuerpo fijo.
- (iv) $\{ f : \mathbb{Q}[i] \rightarrow \mathbb{Q}[i], f \text{ morfismo de cuerpos} \}$.
- (v) $\{ f : \mathbb{Q}[i] \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos} \}$.
- (vi) $\{ f : \mathbb{Q}[\sqrt{2}] \rightarrow \mathbb{Q}[\sqrt{3}], f \text{ morfismo de cuerpos} \}$.
- (vii) $\{ f : \mathbb{Q}[\sqrt[3]{2}] \rightarrow \mathbb{Q}[\sqrt[3]{2}], f \text{ morfismo de cuerpos} \}$.
- (viii) $\{ f : \mathbb{C} \rightarrow \mathbb{C}, f \text{ morfismo de cuerpos tal que } f(a) = a \forall a \in \mathbb{R} \}$.
- (ix) $\{ f : \mathbb{R} \rightarrow \mathbb{R}, f \text{ morfismo de cuerpos} \}$.

5. Caracterizar las unidades de los siguientes anillos:

\mathbb{Z} , \mathbb{K} (cuerpo cualquiera), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-5}]$, $A[X]$ (A dominio íntegro), \mathbb{Z}_n .

6. Sea A un dominio íntegro y \mathbb{K} su cuerpo de cocientes. Probar que $f : A \rightarrow \mathbb{K}$ definida por $f(a) = \frac{a}{1}$ es monomorfismo de anillos.
Deducir la equivalencia de las siguientes afirmaciones:
- (i) D es un dominio íntegro.
 - (ii) Existe $f : D \rightarrow \mathbb{K}$ monomorfismo de anillos para algún cuerpo \mathbb{K} .
7. Caracterizar el cuerpo de cocientes de los siguientes dominios de integridad:
 \mathbb{Z} ; $\mathbb{Z}[i]$; $\mathbb{Z}[\sqrt{2}]$; $A[X]$ (A dominio íntegro); \mathbb{K} (\mathbb{K} cuerpo).
8. Sea A un dominio de integridad y sea $a \in A$. Probar que:
- (i) Si a es primo, es irreducible.
 - (ii) Si A es DFU, todo elemento irreducible es primo.
 - (iii) Dar ejemplos de elementos en $\mathbb{Z}[\sqrt{-5}]$ que sean irreducibles pero no primos.
 - (iv) Si A es DFU, $A[(X_i)_{i \in I}]$ es DFU.
 - (v) Si A es principal, es DFU (pero no vale la recíproca).
 - (vi) Si $f : A \rightarrow B$ es isomorfismo de anillos entonces a es irreducible en A si, y sólo si, $f(a)$ es irreducible en B .
9. Probar que si A es un anillo euclideano, es principal.
10. Probar que \mathbb{Z} , $\mathbb{Z}[i]$, \mathbb{K} , $\mathbb{K}[X]$ (\mathbb{K} cuerpo) son anillos euclidianos.
11. Probar que -1 es un cuadrado en \mathbb{Z}_p si, y sólo si, $p = 2$ ó $p = 4k + 1$.
12. Sea $p \in \mathbb{Z}$ primo. Probar que:
- (i) p es irreducible en $\mathbb{Z}[i]$ si, y sólo si, p no es suma de dos cuadrados en \mathbb{Z} .
 - (ii) p es primo en $\mathbb{Z}[i]$ si, y sólo si, $p = 4k + 3$.
 - (iii) p es suma de dos cuadrados (en \mathbb{Z}) si, y sólo si, $p = 2$ ó $p = 4k + 1$.
13. Sea $a + bi \in \mathbb{Z}[i]$ con $b \neq 0$. Probar que $a + bi$ es irreducible en $\mathbb{Z}[i]$ si, y sólo si, $|a + bi| = a^2 + b^2 \in \mathbb{Z}$ es un número primo no congruente a 3 módulo 4.
14. Sean \mathbb{K} un cuerpo y $f \in \mathbb{K}[X]$.
- (i) Probar que $\mathbb{K}[X]/\langle f \rangle$ es un cuerpo si, y sólo si, f es irreducible.
 - (ii) Construir un cuerpo de 9 elementos.
 - (iii) Probar que $\mathbb{R}[X]/\langle X^2 + 1 \rangle \simeq \mathbb{C}$.
 - (iv) Si $f(X) = \prod_{i=1}^n (X - \alpha_i)$ con $\alpha_i \in \mathbb{K}$ todos distintos, se define $g_i := \prod_{i \neq j} (X - \alpha_j)$; $1 \leq i \leq n$. Probar que $\{\bar{g}_1, \dots, \bar{g}_n\}$ es una base de $\mathbb{K}[X]/\langle f \rangle$ como \mathbb{K} -espacio vectorial y, si $h \in \mathbb{K}[X]$, determinar las coordenadas en esta base de $\bar{h} \in \mathbb{K}[X]/\langle f \rangle$.

15. Sea $f(X) = a_n X^n + \dots + a_0 \in \mathbb{K}[X]$ con $a_n \neq 0$.

Se puede escribir:

$$\begin{aligned} f(X) &= (a_n X^{n-1} + \dots + a_1)X + a_0 \\ &= ((a_n X^{n-2} + \dots + a_2)X + a_1)X + a_0 \\ \dots &= ((\dots((a_n X + a_{n-1})X + a_{n-2})X + \dots)X + a_1)X + a_0. \end{aligned}$$

Es decir, si se define inductivamente:

$$\begin{aligned} H_n &= a_n \\ H_{n-1} &= H_n X + a_{n-1} \\ H_{n-2} &= H_{n-1} X + a_{n-2} \\ &\vdots \\ H_0 &= H_1 X + a_0 \end{aligned}$$

entonces, $H_0 = f$ y $\text{gr}(H_{n-i}) = i$ ($0 \leq i \leq n$).

- (i) Probar que $\{\overline{H}_n, \dots, \overline{H}_1\}$ es una base de $\mathbb{K}[X]/\langle f \rangle$. (Los polinomios H_i se llaman los polinomios de Horner y verifican que calcular H_{n-1}, \dots, H_0 sucesivamente, es la forma de evaluar un polinomio f general en una variable que usa la menor cantidad de productos).
- (ii) Sea $\mu_X : \mathbb{K}[X]/\langle f \rangle \rightarrow \mathbb{K}[X]/\langle f \rangle$ la transformación lineal "multiplicar por X " en $\mathbb{K}[X]/\langle f \rangle$, o sea $\mu_X(\overline{g}) = \overline{Xg}$.
Escribir la matriz de μ_X en la base $\{\overline{H}_n, \dots, \overline{H}_1\}$.
- (iii) Determinar el polinomio característico de la transformación lineal μ_X .

16. Sea p un número primo, y $\Phi : \mathbb{Z}[X] \rightarrow \mathbb{Z}_p[X]$ definida por :

$$\Phi(a_n X^n + \dots + a_0) = \overline{a_n} X^n + \dots + \overline{a_0}$$

(donde $\overline{a_i}$ es el resto de a_i módulo p).

- (i) Probar que $\Phi(f) + \Phi(g) \equiv \Phi(f + g) \pmod{p}$ y $\Phi(f)\Phi(g) \equiv \Phi(fg) \pmod{p}$
- (ii) Sea $f \in \mathbb{Z}[X]$ tal que $\Phi(f) \neq 0$ y $\text{gr} \Phi(f) = \text{gr} f$. Probar que si $\Phi(f)$ es irreducible en $\mathbb{Z}_p[X]$, entonces f no se factoriza en $\mathbb{Z}[X]$ en la forma $f = gh$ con g, h de grado ≥ 1 .

17. *Criterio de Irreducibilidad de Eisenstein.* Sean A un DFU, \mathbb{K} su cuerpo de cocientes y $f = a_n X^n + a_{n-1} X^{n-1} + \dots + a_0 \in A[X]$. Si existe un primo $p \in A$ que verifica que $p \nmid a_n$, $p \mid a_i$ ($0 \leq i \leq n-1$) y $p^2 \nmid a_0$ entonces f es irreducible en $\mathbb{K}[X]$.

18. Sea $p \in \mathbb{Z}$ primo. Probar que:

- (i) $(X+1)^p - 1$ es divisible por X y $\frac{(X+1)^{p-1} - 1}{X} = \sum_{k=0}^{p-1} \binom{p}{k} X^{p-1-k}$ es irreducible en $\mathbb{Q}[X]$.
- (ii) $1 + X + X^2 + \dots + X^{p-1}$ es irreducible en $\mathbb{Q}[X]$.
- (iii) Si $a \in \mathbb{Z}$ es tal que $p \nmid a$ pero $p^2 \nmid a$, entonces $X^n - a$ es irreducible en $\mathbb{Q}[X]$.

19. Mostrar que $X^4 - X^2 + 1$ es irreducible en $\mathbb{Q}[X]$ y factorizar $X^5 + X^4 + X^2 + X + 2$ en $\mathbb{Q}[X]$.
20. Sea $f \in \mathbb{K}[X]$ y sea a una raíz de f en \mathbb{K} . Probar que a es raíz múltiple de f si, y sólo si, es raíz de su derivado.
21. Sea $f \in \mathbb{K}[X]$, con $\mathbb{K} = \mathbb{C}, \mathbb{R}$ ó \mathbb{Q} . Probar que el polinomio $\frac{f}{\text{mcd}(f, f')} \in \mathbb{K}[X]$ tiene las mismas raíces que f en \mathbb{C} , pero todas simples (se lo llama el *polinomio libre de cuadrados asociado a f*).
22. Probar que si $f \in \mathbb{Q}[X]$ es irreducible, no tiene raíces múltiples en \mathbb{C} .
23. Probar que $\sum_{i=0}^n X^i$ y $\sum_{i=0}^n \frac{X^i}{i!}$ no tienen raíces múltiples en \mathbb{C} .
24. Sea $f = aX^2 + bX + c = a(X - \alpha)(X - \beta) \in \mathbb{C}[X]$ con $a \neq 0$.

- (i) Verificar que el *Discriminante* $\Delta := b^2 - 4ac$ también es igual a $a^2(\alpha - \beta)^2$ y reencontrar "f tiene una raíz doble $\Leftrightarrow \Delta = 0$ ".
- (ii) Comparar $\text{Res}_X(f, f')$ con Δ y justificar la afirmación " $\text{Res}_X(f, f') = 0 \Leftrightarrow \Delta = 0$ ".

25. Sea $f = X^3 + pX + q = (X - \alpha)(X - \beta)(X - \gamma) \in \mathbb{C}[X]$.

Se define el *Discriminante* de f como $\Delta(f) = (\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2$. Se verifica que $\Delta(f) = 0 \Leftrightarrow f$ tiene una raíz múltiple.

- (i) Verificar que $\Delta(f) = -4p^3 - 27q^2$. (Observar que $\Delta(f)$ es simétrico en las raíces y, por lo tanto, es un polinomio en los coeficientes de f).
- (ii) Calcular $\text{Res}_X(f, f')$ y comparar con $\Delta(f)$.

26. Sea $f = a_0X^n + \dots + a_n = a_0(X - \alpha_1) \dots (X - \alpha_n) \in \mathbb{C}[X]$, con $a_0 \neq 0, n \geq 2$.

Se define el *Discriminante* de f como:

$$\Delta(f) := a_0^{2n-2} \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

Probar que $\text{Res}_X(f, f') = a_0^{n-1} \prod_i f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} a_0 \Delta(f)$.

27. Determinar todos los polinomios irreducibles de grado 2, 3, 4 y 5 en $\mathbb{Z}_2[X]$.

28. Sea $f = a_nX^n + \dots + a_0 \in \mathbb{C}[X]$, con $a_n \neq 0$, y sea $M := 1 + \left| \frac{a_{n-1}}{a_n} \right| + \dots + \left| \frac{a_0}{a_n} \right|$.

- (i) Probar que si $\alpha \in \mathbb{C}$ es raíz de f , entonces $|\alpha| < M$.

- (ii) Probar que si $f \in \mathbb{R}[X]$, entonces

$$f(M) > 0 \iff a_n > 0 \quad \text{y} \quad f(-M) > 0 \iff (-1)^n a_n > 0.$$

Polinomios en varias variables (Optativos)

29. Sean $f, g \in \mathbb{K}[X_1, \dots, X_n]$. Probar que:
- (i) $f + g = 0$ ó $\text{gr}(f + g) \leq \max\{\text{gr}f, \text{gr}g\}$
 - (ii) $fg = 0 \Rightarrow f = 0$ ó $g = 0$. (Es decir, $\mathbb{K}[X_1, \dots, X_n]$ es un dominio íntegro)
 - (iii) $\text{gr}(fg) = \text{gr}f + \text{gr}g$. (Sug: descomponer a f y g en suma de polinomios homogéneos.)
 - (iv) Cuáles son los elementos inversibles de $\mathbb{K}[X_1, \dots, X_n]$?
 - (v) Probar que $\mathbb{K}[X_1, \dots, X_n]$ tiene una estructura de \mathbb{K} -espacio vectorial y exhibir una base.
 - (vi) Un polinomio de grado d en una variable tiene, a lo sumo, $d + 1$ coeficientes no nulos o monomios. Cuántos coeficientes no nulos puede tener un polinomio de grado d en 2 variables?
 - (vii) Cuántos coeficientes no nulos puede tener un polinomio homogéneo de grado d en n variables?
 - (viii) Cuántos coeficientes no nulos puede tener un polinomio cualquiera de grado d en n variables?
 - (ix)Cuál es la dimensión del \mathbb{K} -espacio vectorial $\mathbb{K}[X_1, \dots, X_n]_{\leq d} = \{f \in \mathbb{K}[X_1, \dots, X_n] : f = 0 \text{ ó } \text{gr}f \leq d\}$.
 - (x) Cuáles son los polinomios irreducibles de $\mathbb{K}[X_1, \dots, X_n]$?
30. Mostrar que $X^2 + Y^2 - 1$ y $XT - YZ$ son irreducibles en $\mathbb{Q}[X, Y]$ y $\mathbb{Q}[X, Y, Z, T]$ respectivamente.
31. (i) Probar que si un polinomio $f \in \mathbb{C}[X_1, \dots, X_n]$ se anula sobre todos los puntos de \mathbb{Z}^n entonces f es el polinomio nulo.
- (ii) Probar que pasa lo mismo si f se anula en $\{(x_1, \dots, x_n) \in \mathbb{Z}^n : 0 \leq x_i \leq \text{gr}f, 1 \leq i \leq n\}$.
32. Sean $f = XY - 1$ y $g = X^2 + Y^2 - 4$. Mirando f y g como polinomios en X a coeficientes en Y , calcular $\text{Res}_X(f, g)$. Tienen f y g un factor en común en $\mathbb{Q}[X, Y]$? Y en $\mathbb{Q}(Y)[X]$?
33. Sea $I = \langle Y + X^2 - 1, XY - 2Y^2 + 2Y \rangle \subset \mathbb{R}[X, Y]$.
- (i) Determinar una base del \mathbb{R} -espacio vectorial $\mathbb{R}[X, Y]/I$.
 - (ii) Determinar un isomorfismo entre $\mathbb{R}[X, Y]/I$ y \mathbb{R}^n para algún $n \in \mathbb{N}$.
 - (iii) Decidir si $\mathbb{R}[X, Y]/I$ es un cuerpo.
34. Sea $I = \langle X^2 + Y^5, X^3 + Y^4 \rangle \subset \mathbb{C}[X, Y]$. Decidir si los siguientes pares de polinomios determinan la misma clase en $\mathbb{C}[X, Y]/I$:
- (i) $XY, 1$
 - (ii) XY^5, Y^4
 - (iii) $Y^4, -X^4Y$
 - (iv) $5X^2 + 7Y^2, 5Y^2 + 7X^2$.